

Enterprise Risk Management

Effective enterprise risk management requires clear roles and responsibilities for management, individual board committees, and the Risk Management Committee

Management

- Identify and manage all business risks
- Perform risk assessments on all identified risks
- Develop risk appetite recommendations for respective risks for board approval
- Develop, implement, and manage risk mitigations and controls
- Identify and monitor emerging risks
- Provide assurance to the board regarding effectiveness of risk mitigations and controls

Board Committees

- Oversee all risks relating to the committee's responsibilities:
 - Establish risk appetite for respective areas
 - Review management's risk assessments and assurances
 - Review risk mitigations and controls to oversee that risk exposures remain within risk appetites
 - Monitor emerging risks
- Liaise with other committees regarding overlapping risk implications

Risk Management Comm.

- Approve* the risk policy framework, including enterprise risk strategies
- Establish overall enterprise risk appetite
- Oversee the consistency and effectiveness of enterprise risk management processes and capabilities
- Confirm board committees are providing appropriate risk oversight
- Oversee aggregate risk exposure and prioritization
- Oversee independent reassurance of management's reports and controls
- Oversee risks which are the responsibility of the full board (cross-functional)

*Note: "Approve" means recommend to the full board for approval; with the exception of the Investment Committee, which has final decision authority, committees recommend to the full board and do not have final decision authority.

Board Committee Operations Regarding Risk

The Risk Management Committee will interface primarily with the Chief Risk Officer, while the other committees will interact primarily with executive risk owners from their respective areas

Role of Office of Enterprise Risk Management

- Develop the policies for enterprise risk strategies and risk appetite
- Develop the enterprise risk framework and tools to improve enterprise risk management processes and capabilities
- Prioritize risks and provide assessments of aggregate enterprise risk exposure
- Provide independent reassurance on the reliability of management's risk assessments, mitigations, and controls
- Integrate risk assessments, enterprise compliance, enterprise privacy and security, investigations, and training and awareness

Primary Committee Interface

**Risk
Management
Committee**

Role of Executive Risk Owners

- Identify, assess, and manage all business risks
- Develop risk appetite recommendations for each risk area
- Develop, implement and manage risk mitigations and controls
- Identify and monitor emerging risks
- Provide assurance to the board regarding effectiveness of risk mitigations and controls

**BPAC
Finance
Governance
Health
Benefits
Investment
Perf. & Comp.**

Example Board Committee Risk Responsibility Map

Mapping Approach:

- Each subcategory of risks maps to the board committee whose delegated authority aligns most closely
- Where risks span several committees, the Risk Management Committee is responsible

Category	Subcategory	BPAC	Finance	Health Benefits	Perf and Comp	Investment	Board Governance	Risk Management	Full Board
Strategic	Health Care Reform			X					
	Health Care PPO Funding			X					
	Health Care Costs			X					
	Long Term Care Program			X					
	Pension Funding	X							
	Pension Reform	X							
	Actuarial	X							
	Governance / Leadership					X	X		
	Strategy and Policy							X	X
	Stakeholder Relations							X	X
Operational	Business Planning		X						
	Organization							X	
	Procurement and Contract Management		X						
	Business Continuity Management		X						
	Performance Management		X						
	Operational Controls		X						
	Technology / Systems Management		X						
	Information Security		X						
	PSR							X	X
	Customer/ Member Service	X							
	Human Resources Management				X				

Illustrative

Responsibilities Example

Example: Procurement and Receiving Risk – Finance Committee

Risk Category	Sub-Category	Specific Risk	Definition	Executive Owner
Operational	Procurement and Contract Management	Procurement and Receiving Risk:	Procurement is not completed on a timely basis. Decentralized purchase order administration, inconsistent levels of purchase order payment authorization, or lack of centralized receiving/ monitoring/ reconciliation process result in receiving and payment risk.	Deputy Executive Officer, Operations and Technology

Management

- Identify, assess, and manage all procurement and receiving process business risks
- Develop, implement and manage procurement and receiving process risk mitigations and controls
- Develop risk appetite recommendations for Procurement and Contract Management
- Identify and monitor emerging procurement and receiving process risks
- Provide assurance to the board regarding procurement and receiving process risk mitigations and controls

Finance Committee

- Oversee all risks relating to Finance Committee responsibilities above an agreed-upon threshold:
 - Review management's risk assessments of the procurement and receiving process
 - Review the consistency and effectiveness of procurement and receiving process risk mitigations and controls
 - Approve the risk appetite for Procurement and Contract Management
 - Monitor emerging contracting process risks
- As appropriate, liaise with other committees regarding procurement and receiving process risk implications

Risk Management Comm.

- Oversee independent reassurance of management's procurement and receiving process risk assessments, reports and controls
- Oversee prioritization of procurement and receiving process risk relative to other enterprise process risks and liaise with other committee chairs, as appropriate

Responsibilities Example

Example: Credit Risk – Investment Committee

Risk Category	Sub-Category	Specific Risk	Definition	Executive Owner
Investments	Counterparty Exposure	Credit Risk	The exposure to actual loss as a result of the default (or other failure to perform) by an economic or legal entity with which CalPERS does business; usually refers to a bad debt possibility.	Chief Investment Officer

Management

- Identify, assess, and manage all credit business risks
- Develop, implement and manage credit risk mitigations and controls
- Develop risk appetite recommendations for Counterparty Exposure
- Identify and monitor emerging credit risks
- Provide assurance to the board regarding credit risk mitigations and controls

Investment Committee

- Oversee all risks relating to Investment Committee responsibilities above an agreed-upon threshold:
 - Review management’s risk assessments of credit
 - Review the consistency and effectiveness of credit risk mitigations and controls
 - Approve the risk appetite for Counterparty Exposure
 - Monitor emerging credit risks
- As appropriate, liaise with other committees regarding credit risk implications

Risk Management Comm.

- Oversee independent reassurance of management’s credit risk assessments, reports and controls
- Oversee prioritization of credit risk relative to other enterprise process risks and liaise with other committee chairs, as appropriate

Responsibilities Example

Example: PSR – Risk Management Committee

Risk Category	Sub-Category	Specific Risk	Definition	Executive Owner
Operational	PSR	PSR	PSR implementation could cause significant impacts to customer service levels, staff workload capacity, and information security.	Deputy Executive Officer, Operations and Technology

Management

- Identify, assess, and manage all PSR process business risks
- Develop, implement and manage PSR process risk mitigations and controls
- Develop risk appetite recommendations for PSR
- Identify and monitor emerging PSR process risks
- Provide assurance to the board regarding effectiveness of PSR risk mitigations and controls

Risk Management Comm.

- Oversee all risks relating to Risk Management Committee responsibilities above an agreed-upon threshold:
 - Review management's assessments of PSR risks
 - Review the consistency and effectiveness of PSR risk mitigations and controls
 - Approve the risk appetite for PSR
 - Monitor emerging PSR risks
- As appropriate, liaise with other committees regarding PSR risk implications
- Oversee independent reassurance of management's PSR risk assessments, reports and controls
- Oversee prioritization of PSR risk relative to other enterprise process risks and liaise with other committee chairs, as appropriate

Full Board

- Provide oversight of impact to aggregate risk level
- Ensure management is adequately managing risks
- Receives reports from the Risk Management Committee
- Oversee independent reassurance of management's PSR risk assessments, reports and controls